# IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | | |
|---|---|---|
| Appellant: Lu, et al. | § | Group Art Unit: 2444 |
| Application No.: 10/593,314 | § | Examiner: Farrukh Hussain |
| § 371(c) Date: April 17, 2007 | § | Confirmation No.: 7532 |
| For: METHOD FOR BINDING WORK LABEL SWITCHING PATH AND PROTECTION LABEL SWITCHING PATH | § | |

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**CERTIFICATE OF EFS-WEB FILING**

Pursuant to 37 C.F.R. §1.8, I hereby certify that this correspondence is being electronically submitted to the U.S. Patent and Trademark Office website, www.uspto.gov, on February 15, 2011

Jerri Pearson

## APPEAL BRIEF

Dear Sirs:

This Appeal Brief is filed in support of the appeal in the above-referenced application and is filed pursuant to the Notice of Appeal filed February 3, 2010. The Appellant authorizes all required fees under 37 C.F.R. § 1.17 to be charged to Deposit Account No. 50-1515, of Conley Rose, P.C. of Texas.

# TABLE OF CONTENTS

## I. REAL PARTY IN INTEREST

The real party in interest in the present application is the following party: Huawei Technologies Co., Ltd.

## II. RELATED APPEALS AND INTERFERENCES

None.

## III. STATUS OF CLAIMS

### A. Total Number of Claims in the Application

Claims in the application: 1-19.

### B. Status of All Claims in the Application

1. Claims canceled: None.
2. Claims withdrawn from consideration but not canceled: None.
3. Claims pending: 1-19.
4. Claims allowed: None.

6. Claims objected to: None.

5. Claims rejected: 1-19.

### C. Claims on Appeal

Claims on appeal: 1-19.

## IV. STATUS OF AMENDMENTS

There are not any outstanding claim amendments.

## V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Multiprotocol Label Switching (MPLS) is a data transport technique in which data is transmitted through the network according to predefined paths made up of various physical components of the network. These pre-defined paths are referred to as work label switching paths (work LSP). To assure that the MPLS network can work properly even when some nodes of the work LSP fails, a protection label switching path (protection LSP) is provided to transport data instead of work LSP when the work LSP fails. Depending on the protection mode, the protection LSP may or may not be used to carry data when the work LSP is operation.

Two nodes (e.g., a source node and a destination node) may have many work LSPs and protection LSP extending between them. As such, each node has to bind each work LSP to at least one of the protection LSPs so that the nodes know which protection LSP to use if the work LSP fails. In the prior art, the work LSP and the protection LSP are usually configured statically and bound together. However, static configuration increases burden of the network administrator.

The present invention provides a method for automatically binding a work LSP with a protection LSP. The binding of work LSP and protection LSP is implemented via signaling transportation in the process of creating the protection LSP.

This section provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by paragraph and line number. Each element of the claims is identified with a corresponding reference to the specification where applicable. The citation to passages in the specification for each claim element does not imply that the limitations from the specification should be read into the corresponding claim element.

Independent claim 1 recites a method for binding a work LSP with a protection LSP, comprising: a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML) to request for creating the protection LSP of the work LSP; *see, e.g.*, specification at p. 5, ll. 26-29; the PML router assigning a label for the protection LSP based on the first message, and returning a second message which comprises the binding information, *see, e.g.*, specification at p. 6, ll. 9-13; upon receiving the second message, the PSL router binding the work LSP with the protection LSP according to the binding information, and transmitting a notification message which comprises the binding information to the PML switched router, *see, e.g.*, specification at p. 6, ll. 14-19; and the PML router binding the work LSP with the protection LSP according to the binding information in the notification message, *see, e.g.*, specification at p. 6, ll. 20-21; wherein the binding information comprises an identifier of the work LSP, a type of the LSP, and a protection mode, *see, e.g.*, specification at p. 6, ll. 5-8; and wherein the PSL and PML are label edge routers, *see, e.g.*, specification at p. 4, ll. 25-29 and p. 5, ll. 1-4.

Independent claim 3 recites a method for binding a work LSP with a protection LSP, comprising: in the process of creating the protection LSP, *see, e.g.*, specification at p. 5, ll. 7-11, a PSL transmitting a first message which comprises a binding information to a PML to request for creating the protection LSP of the work LSP, *see, e.g.*, specification at p. 5, ll. 26-29; the PML router assigning a label for the protection LSP based on the first message, and returning a second message which comprises the binding information, *see, e.g.*, application at specification at p. 6, ll. 9-13; upon receiving the second message, the PSL router binding the work LSP with the protection LSP according to the binding information, and transmitting a notification message which comprises the binding information to the PML switched router *see, e.g.*, specification at p.

6, ll. 14-19; and the PML router binding the work LSP with the protection LSP according to the binding information in the notification message *see, e.g.*, specification at p. 6, ll. 20-21, if the protection mode for the work LSPs is 1+1 mode, the binding information comprises the work LSP identifier, LSP type, and the protection mode; and if the protection mode for the work LSPs is 1:1, the binding information comprises the work LSP identifier, LSP type, the protection mode and selection mode of the return LSP in the 1:1 protection mode *see*, *e.g.*, specification at p. 6, ll. 5-8 .

## VI. GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-19 are rendered obvious under 35 U.S.C. § 103(a) by the combination of U.S. Patent Application Publication 2004/0004955 (*Lewis*), U.S. Patent Application Publication 2002/0116669A1 (*Jain*), and U.S. Patent 7,315,510 (*Owens*).

## VII. ARGUMENTS

### A. To render obvious claims 4, 5, 8, 13, 14, 21, and 28, the cited prior art must disclose all of the elements of claims 4, 5, 8, 13, 14, 21, and 28.

Claims 1-19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over *Lewis* in view of *Jain* and *Owens*. Claims 2 and 4-19 depend from independent claim 1. Thus, claims 1-19 stand or fall on the application of the combination of *Lewis*, *Jain*, and *Owens* to independent claims 1 and 3. As noted by the United States Supreme Court in *Graham v. John Deere Co. of Kansas City*, an obviousness determination begins with a finding that **"the prior art as a whole in one form or another contains all of the elements of the claimed invention"**. *See Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 22 (U.S. 1966). The Applicants respectfully

submit that the combination of *Lewis*, *Jain*, and *Owens* does not contain all of the elements of independent claims 1 and 3, and therefore fails to render obvious claims 1-19.

**B. The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP.**

The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP. Claims 1 and 3 read:

> 1. A method for binding a work label switching path (LSP) with a protection LSP, comprising:
>
> **a Path Switching Label Switching Router (PSL) transmitting a first message** which comprises a binding information to a Path Merging Label Switching Router (PML) **to request for creating the protection LSP of the work LSP**;
>
> **the PML router assigning a label for the protection LSP based on the first message**, and returning a second message which comprises the binding information;
>
> upon receiving the second message, the PSL router binding the work LSP with the protection LSP according to the binding information, and transmitting a notification message which comprises the binding information to the PML switched router; and
>
> the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,
>
> wherein the binding information comprises an identifier of the work LSP, a type of the LSP, and a protection mode, and
>
> wherein the PSL and PML are label edge routers.

> 3. A method for binding a work label switching path (LSP) with a protection LSP, comprising:
>
> in the process of creating the protection LSP, **a Path Switching Label Switching Router (PSL) transmitting a first message** which comprises a binding information to a Path Merging Label Switching Router (PML) **to request for creating the protection LSP of the work LSP**;
>
> **the PML router assigning a label for the protection LSP based on the first message**, and returning a second message which comprises the binding information;
>
> upon receiving the second message, the PSL router binding the work LSP with the protection LSP according to the binding information, and transmitting a notification message which comprises the binding information to the PML switched router; and
>
> the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,
>
> if the protection mode for the work LSPs is 1+1 mode, the binding information comprises the work LSP identifier, LSP type, and the protection mode; and
>
> if the protection mode for the work LSPs is 1:1, the binding information comprises the work LSP identifier, LSP type, the protection mode and selection mode of the return LSP in the 1:1 protection mode.

(Emphasis added). As shown above, claims 1 and 3 require that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP. Initially, the Examiner asserted that *Jain's* paragraph 5 discloses that the PML router **assigns a label for the protection LSP** based on a message requesting creation of the protection LSP for the work LSP. *See* Office Action dated October 6, 2010 (*Final Office Action*), pp. 5-6. However, the cited section of *Jain* describes how *Jain* modifies **the packet** by exchanging the **outgoing label** for the **prior label before forwarding the packet along this next hop**, rather than **assigning a label for the protection LSP**:

> **A label associated with a data packet** identifies the appropriate next hop for the packet along the predefined path. At the nodes, a forwarding table (also referred to as a label-swapping table) associates incoming labels with appropriate outgoing labels. When a node receives a data packet, the forwarding table is used to look up the packet label. The corresponding entry indicates a next hop for the packet and provides the outgoing label. **The router then modifies the packet by exchanging the outgoing label for the prior label before forwarding the packet along this next hop.**

*Jain*, ¶ 5 (emphasis added). As shown above, *Jain's* paragraph 5 describes how *Jain's* router modifies the **packet** by exchanging the outgoing label for the prior label before forwarding the packet along this next hop. Adding a label to a packet is not the same as assigning a label for the protection LSP. More specifically, claims 1 and 3 require a label to be assigned to the protection LSP (indicating that there was previously no association between the label and the protection path), whereas *Jain* adds an existing label to the packet (indicating a previously existing relationship between the label and the protection path). Regardless, **the cited section of *Jain* never discloses that the label is added to the packet in response to a label creation request**. Thus, *Jain's* paragraph 5 fails to disclose that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP.

Subsequently, the Examiner asserted that *Jain's* paragraph 100 discloses that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP. *See* Advisory Action dated January 4, 2011 (*Advisory Action*), p. 2. However, the cited section of *Jain* describes how *Jain*: (1) responds to a message indicating failure of the work LSP, not a message requesting creation of a protection LSP, and (2) adds the next hop label 802 to the packet as the appropriate label for the next hop for the appropriate protection LSP that corresponds to the shared resource link group (SRLG), not assigning a label for the protection LSP:

> Program flow may then move from the state 626 to a state 628. In the state 628, data traversing **a protected LSP that is experiencing the fault identified in the notification received in the state 626** may be re-routed via one of the protection LSPs so to avoid the fault. Each node may then determine whether the fault affects its applications (e.g., LSPs or IGP communications that the node is using). For example, the fault manager 336 (FIG. 3) of each node may then look up the SRLG its forwarding table 312 (FIG. 3) to determine whether any LSPs associated with the node are affected by the fault. If so, then the next hop label 802 (FIG. 8) identified based on the SRLG may be substituted and used as the appropriate label **for the next hop** for the appropriate protection LSP that corresponds to the SRLG. Accordingly, the protected LSP is reformed using the protection LSP to avoid the fault. Program flow for the identified fault may terminate in the state 630.

*Jain*, ¶ 100 (emphasis added). As shown above, the cited section of *Jain* describes how *Jain* responds to a message indicating failure of the work LSP, not a message requesting creation of a protection LSP. **A message indicating a failure of the work LSP is not the same as a message requesting creation of a protection LSP**. In addition, the cited section of *Jain* describes how *Jain* adds the next hop label 802 to the packet as the appropriate label for the next hop for the appropriate protection LSP that corresponds to the SRLG, not assigning a label for the protection LSP. **The addition of a label for the next hop for the protection LSP to the packet is not the same as assigning a label for the protection LSP**. Thus, *Jain's* paragraph 100 fails to disclose that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP. *Lewis* and *Owens* fail to make up for the deficiencies of *Jain*. Therefore, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the PML router assigns a label for the protection LSP based on a message requesting creation of the protection LSP for the work LSP. As such, the combination of *Lewis*, *Jain*, and *Owen* fails to disclose at least one limitation of independent claims 1 and 3, and consequently fails to render obvious claims 1-19.

### C. The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise an identifier of the work LSP.

The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise an identifier of the work LSP. Claims 1 and 3 read:

> 1. A method for binding a work label switching path (LSP) with a protection LSP, comprising:
>
> **a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML)** to request for creating the protection LSP of the work LSP;
>
> **the PML router** assigning a label for the protection LSP based on the first message, and **returning a second message which comprises the binding information**;
>
> upon receiving the second message, **the PSL router** binding the work LSP with the protection LSP according to the binding information, and **transmitting a notification message which comprises the binding information to the PML switched router**; and
>
> the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,
>
> **wherein the binding information comprises an identifier of the work LSP**, a type of the LSP, and a protection mode, and
>
> wherein the PSL and PML are label edge routers.

3. A method for binding a work label switching path (LSP) with a protection LSP, comprising:

in the process of creating the protection LSP, **a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML)** to request for creating the protection LSP of the work LSP;

**the PML router** assigning a label for the protection LSP based on the first message, and **returning a second message which comprises the binding information**;

upon receiving the second message, **the PSL** router binding the work LSP with the protection LSP according to the binding information, and **transmitting a notification message which comprises the binding information to the PML switched router**; and

the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,

if the protection mode for the work LSPs is 1+1 mode, **the binding information comprises the work LSP identifier**, LSP type, and the protection mode; and

if the protection mode for the work LSPs is 1:1, **the binding information comprises the work LSP identifier**, LSP type, the protection mode and selection mode of the return LSP in the 1:1 protection mode.

(Emphasis added). As shown above, claims 1 and 3 require that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise an identifier of the work LSP. Initially, the Examiner asserted that *Owens's* col. 11, ll. 1-12 discloses that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise an identifier of the work LSP. *See Final Office Action*, p. 7. However, the cited section of *Owens* discloses the identification of a **protection switch or node**, not the work LSP:

> A Protection Domain Path is established by the **identification of a protection switch or node and an end point switch or node in the MPLS network.** The protection switch element ("PSL") initiates the setup of the working LSP and elements and the recovery LSP and elements. It is also responsible for storing information about which network switch elements or portions thereof have protection enabled, and for maintaining a binding between outgoing labels specifying the working path and the protection/recovery path. The latter enables the switchover to the recovery path upon the receipt of a protection switch trigger.

*Owens*, col. 11, ll. 2-12 (emphasis added). As shown above, the cited section of *Owens* discloses the **identification of a protection switch or node** and an end point switch or node in the MPLS network. In contrast, claims 1 and 3 require that the binding information comprise **an identifier of the work LSP**. Since many work and protection LSPs may extend from a single switch or node, the identification of an endpoint switch or node is insufficient to identify a specific LSP. Even if only one LSP extended form a node (and without conceding such), Jain identifies the **protection** node, not the **work** node. Thus, *Owens's* col. 11, ll. 2-12 fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise an identifier of the work LSP.

The Examiner also initially asserted that *Jain's* paragraphs 21 and 106 disclose label binding information comprising an identifier of the work LSP. *See Final Office Action*, p. 11. However, **the cited sections of *Jain* fail to disclose that the fault notification message contains any label binding information**, much less the identifier of the work LSP:

> The network may be a label-switching network. Label switching may be performed in accordance with MPLS. **Propagation of a fault notification label may be by an interior gateway protocol (IGP). Propagation of the fault notification may include sending the fault notification by a label switched packet. The label switched packet may have a fault information label (FIL) that distinguishes the fault notification from data traffic.** A substantially same FIL may be sent with each fault notification regardless of which network node originates the fault notification. Or, each network node may originate fault notifications having a FIL that is unique to the node. Network nodes that would be affected by the corresponding point of failure may store the indicia of the identified possible points of failure. The network nodes that would be affected by the corresponding point of failure may set up a label-switched path that uses a resource identified by the corresponding point of failure. At least one of the network nodes that receives a fault notification that corresponds to a point of failure that affects operation of the node may recover from the fault.

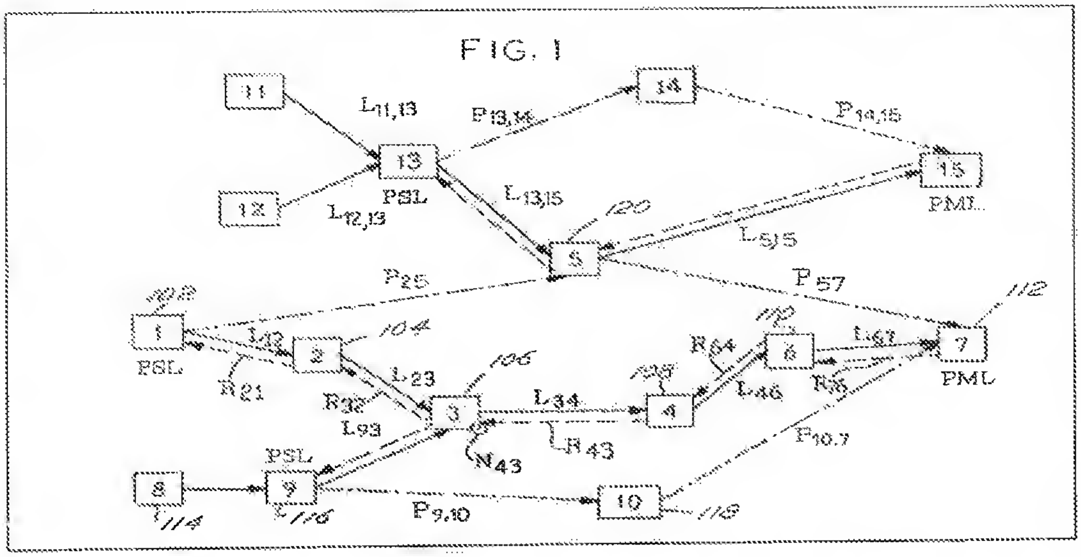
> Then, program flow moves to a state 906 in which a level or type of protection criteria for the resource identified in the state 904 may be specified. This criteria may, for example, specify a level of redundancy available to the resource. The level or kind of criteria specified in the state 906 will generally result from the topology of the network and from characteristics of individual network elements. For example, the protection provided may be 1:1, 1:n, 1+1, ring, or fast re-route. Fast re-route may be as explained above in reference to FIGS. 6-8 or another fast re-routing technique. Further, these criteria may be further specified according to classes and sub-classes of protection. For example, 1:1 protection may be considered a special case of 1:n protection that provides a higher level of fault tolerance than other 1:n levels.

*Jain*, ¶¶ 21 & 106 (emphasis added). As shown above, *Jain's* fault notification message comprises a fault information label (FIL) that **identifies the fault notification message**, not the work LSP. Thus, *Jain's* paragraphs 21 and 106 fail to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise an identifier of the work LSP.

Subsequently, the Examiner asserted that *Owens's* col. 2, ll. 44-54 discloses that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise an identifier of the work LSP. *See Advisory Action*, p. 2. However, the cited section of *Owens* contains no such disclosure:

> In an MPLS data network comprised of various transmission media linking various types of switching systems, network fault recovery time is reduced by using a reverse-directed status message that is generated by a data switch that is down-stream from a switching system from which data is received. The reverse-directed or upstream status message is sent over a pre-determined pathway (i.e. through pre-determined switches and/or over pre-determined data links) which originates from a destination switch or node in an MPLS network to upstream switching systems. This so-called reverse notification tree carries a message or messages that are used to indicate the functionality (or non-functionality) of the downstream switch, switches or links of the MPLS network. As long as an upstream MPLS switching system continues to receive the reverse-directed status message from a downstream switch via the reverse notification tree, the switching systems that receive such a message consider the downstream switch and pathways to be in intact. Accordingly, data packets continue to be sent downstream for subsequent routing and/or processing. If the reverse-directed status message is lost or discontinued, either because of a switch failure or a link failure, the upstream switching system considers the downstream switch or link to have failed and thereafter begins executing a procedure by which data is rerouted over an alternate data path through the network. In the preferred embodiment, the alternate data path over which downstream information [is] sent is a pre-established protection path and is known to a protection switch in advance, thereby minimizing data loss attributable to the time it might take to calculate a dynamic alternate protection path.

*Owens*, col. 2, ll. 27-57 (emphasis added). As shown above, the cited section of *Owens* does not disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise an identifier of the work LSP. The Examiner also asserted that switches 2, 3, 4, 6, and 7 identified by reference numerals 104, 106, 108, 110, and 112, respectively, were relevant to his analysis. *Owens's* FIG. 1 and col. 3, ll. 44-67 disclose switches 2, 3, 4, 6, and 7 identified by reference numerals 104, 106, 108, 110, and 112, respectively:




In routing data between switch no. 1 (represented by reference numeral 102) and switch no. 7 (represented by reference numeral 112) data might be routed between these two endpoints through a "primary" path that is comprised of links that logically or physically couple **switches 2, 3, 4, 6 and 7 (identified by reference numerals 104, 106, 108, 110 and 112 respectively)**. The physical or logical links of the primary path between the endpoints which is 1 and 7 are represented by the vectors designated $L_{12}$, $L_{23}$, $L_{34}$, $L_{46}$ and $L_{67}$. This path is known in the art as the working or primary path through the network. The links of the various paths shown in FIG. 1 (represented by the vectors $L_{12}$, $L_{23}$, $L_{34}$, $L_{46}$ and $L_{67}$), and therefore the paths themselves, might be constructed of direct pathways (e.g., fiber optic cable, coaxial cable, unshielded twisted pairs of copper wires, or microwave radio) between the various switches. Alternate embodiments of the paths or links between switches of the network of FIG. 1 would also include using direct pathways, and intermediate switches or switch networks, (not shown in FIG. 1, but still part of the path or link coupling one or more switching systems to another). By way of example and not of limitation, the data switches shown in FIG. 1 might be IP switches but such IP switches could be linked together using one or more ATM switches or ATM networks.

*Owens*, FIG. 1 & col. 3, ll. 44-67 (emphasis added). As shown above, **the cited section of *Owens* merely discloses the existence of the switches associated with the primary LSP, not that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise an identifier of the work LSP**. Even if the cited section of *Owens* disclosed that the binding information in the various messages comprises the switches associated with the primary LSP (and without conceding such),

*Owens's* identifier is identifier of **switches** of the primary path, not **an identifier of the work LSP** (i.e., the path) contained in the binding information. **Since the switches can support multiple paths between each other, identifying only the switches will not uniquely identify the path**. Thus, the cited sections of *Owens* fail to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise an identifier of the work LSP. *Lewis* and *Jain* fail to make up for the shortcomings in *Owens*. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose at least one limitation of claims 1 and 3, and consequently fails to render obvious claims 1-19.

**D. The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP.**

The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP. Claims 1 and 3 read:

1. A method for binding a work label switching path (LSP) with a protection LSP, comprising:

**a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML)** to request for creating the protection LSP of the work LSP;

**the PML router** assigning a label for the protection LSP based on the first message, and **returning a second message which comprises the binding information**;

upon receiving the second message, **the PSL router** binding the work LSP with the protection LSP according to the binding information, and **transmitting a notification message which comprises the binding information to the PML switched router**; and

the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,

**wherein the binding information comprises** an identifier of the work LSP, **a type of the LSP**, and a protection mode, and

wherein the PSL and PML are label edge routers.

3. A method for binding a work label switching path (LSP) with a protection LSP, comprising:

in the process of creating the protection LSP, **a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML)** to request for creating the protection LSP of the work LSP;

**the PML router** assigning a label for the protection LSP based on the first message, and **returning a second message which comprises the binding information**;

upon receiving the second message, **the PSL** router binding the work LSP with the protection LSP according to the binding information, and **transmitting a notification message which comprises the binding information to the PML switched router**; and

the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,

if the protection mode for the work LSPs is 1+1 mode, **the binding information comprises the** work LSP identifier, **LSP type**, and the protection mode; and

if the protection mode for the work LSPs is 1:1, **the binding information comprises** the work LSP identifier, **LSP type**, the protection mode and selection mode of the return LSP in the 1:1 protection mode.

(Emphasis added). As shown above, claims 1 and 3 require that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP. Initially, the Examiner asserted that *Owens's* col. 6, ll. 33-

43 discloses that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP. *See Final Office Action*, p. 7. However, the cited section of *Owens* merely describes how the format of *Owens's* liveness message[1] depends on the type of network:

> As set forth above, the format of a liveness message will depend upon **the type of switching systems used in the network. IP switches and ATM switches will need to comply with their respective protocols**. Alternative embodiments of the invention would certainly contemplate other sorts of liveness messages having different formats with the salient feature of the message being that the message indicates to an upstream switch that downstream directed data messages were received by a downstream switch intact.

*Owens*, col. 6, ll. 33-43 (emphasis added). As shown above, the cited section of *Owens* merely describes how the format of *Owens's* liveness message depends on the type of network, not that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise **the type of LSP**. Thus, *Owens's* col. 6, ll. 33-43 fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP.

The Examiner also initially asserted that *Jain's* paragraphs 21 and 106 disclose label binding information comprising a type of the LSP. *See Final Office Action*, p. 11. However, **the cited sections of *Jain* fail to disclose that the fault notification message contains any label binding information**, much less the type of the LSP:

[1] *Owens* defines his liveness message as a message that, when lost, indicates a pathway failure. *See Owens*, col. 4, l. 55 – col. 5, l. 6.

> The network may be a label-switching network. Label switching may be performed in accordance with MPLS. Propagation of a fault notification label may be by an interior gateway protocol (IGP). Propagation of the fault notification may include sending the fault notification by a label switched packet. The label switched packet may have a fault information label (FIL) that distinguishes the fault notification from data traffic. A substantially same FIL may be sent with each fault notification regardless of which network node originates the fault notification. Or, each network node may originate fault notifications having a FIL that is unique to the node. Network nodes that would be affected by the corresponding point of failure may store the indicia of the identified possible points of failure. The network nodes that would be affected by the corresponding point of failure may set up a label-switched path that uses a resource identified by the corresponding point of failure. At least one of the network nodes that receives a fault notification that corresponds to a point of failure that affects operation of the node may recover from the fault.
>
> Then, program flow moves to a state 906 in which a level or type of protection criteria for the resource identified in the state 904 may be specified. This criteria may, for example, specify a level of redundancy available to the resource. The level or kind of criteria specified in the state 906 will generally result from the topology of the network and from characteristics of individual network elements. For example, the protection provided may be 1:1, 1:n, 1+1, ring, or fast re-route. Fast re-route may be as explained above in reference to FIGS. 6-8 or another fast re-routing technique. Further, these criteria may be further specified according to classes and sub-classes of protection. For example, 1:1 protection may be considered a special case of 1:n protection that provides a higher level of fault tolerance than other 1:n levels.

*Jain*, ¶¶ 21 & 106. As shown above, the cited sections of *Jain* fail to disclose any messages comprising the type of LSP. Thus, *Jain's* paragraphs 21 and 106 fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP.

Subsequently, the Examiner asserted that *Owens's* col. 11, ll. 54-67 discloses that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP. *See Advisory Action*, p. 2. However, the cited section of *Owens* merely describes one type of LSP (an LSP tunnel),

not that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP:

> Hosts and routers that support both RSVP and Multi-Protocol Label Switching can associate labels with RSVP flows. When MPLS and RSVP are combined, the definition of a flow can be made more flexible. Once a label switched path (LSP) is established, the traffic through the path is defined by the label applied at the ingress node of the LSP (label switched path). The mapping of a label to traffic can be accomplished using a number of different criteria. The set of packets that are assigned the same label value by a specific node are said to belong to the same forwarding equivalence class (FEC) and effectively define the "RSVP flow." **When traffic is mapped onto a label-switched path in this way, we call the LSP an "LSP Tunnel"**. When labels are associated with traffic flows, it becomes possible for a router to identify the appropriate reservation state for a packet based on the packet's label value.

*Owens*, col. 11, l. 55 – col. 12, l. 2 (emphasis added). As shown above, the cited section of *Owens* merely describes one type of LSP (an LSP tunnel), not that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP. Thus, *Owens* fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP. *Lewis* and *Jain* fail to make up for the shortcomings in *Owens*. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose at least one limitation of claims 1 and 3, and consequently fails to render obvious claims 1-19.

### E. The combination of *Lewis, Jain*, and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis, Jain*, and *Owens* fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the protection mode.

The combination of *Lewis, Jain*, and *Owens* fails to render obvious claims 1-19 because the combination of *Lewis, Jain*, and *Owens* fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the protection mode. Claims 1 and 3 read:

1. A method for binding a work label switching path (LSP) with a protection LSP, comprising:

**a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML)** to request for creating the protection LSP of the work LSP;

**the PML router** assigning a label for the protection LSP based on the first message, and **returning a second message which comprises the binding information**;

upon receiving the second message, **the PSL router** binding the work LSP with the protection LSP according to the binding information, and **transmitting a notification message which comprises the binding information to the PML switched router**; and

the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,

**wherein the binding information comprises** an identifier of the work LSP, a type of the LSP, and **a protection mode**, and

wherein the PSL and PML are label edge routers.

3. A method for binding a work label switching path (LSP) with a protection LSP, comprising:

in the process of creating the protection LSP, **a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML)** to request for creating the protection LSP of the work LSP;

**the PML router** assigning a label for the protection LSP based on the first message, and **returning a second message which comprises the binding information**;

upon receiving the second message, **the PSL** router binding the work LSP with the protection LSP according to the binding information, and **transmitting a notification message which comprises the binding information to the PML switched router**; and

the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,

if the protection mode for the work LSPs is 1+1 mode, **the binding information comprises** the work LSP identifier, LSP type, and **the protection mode**; and

if the protection mode for the work LSPs is 1:1, **the binding information comprises** the work LSP identifier, LSP type, **the protection mode** and selection mode of the return LSP in the 1:1 protection mode.

(Emphasis added). As shown above, claims 1 and 3 require that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the protection mode. Initially, the Examiner asserted that *Owens's* col. 11,

ll. 1-12 discloses that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the protection mode. *See Final Office Action*, p. 7. While the cited section of *Owens* describes how *Owens's* binds work LSPs to protection LSPs, it does not say anything regarding the type of protection mode used:

> A Protection Domain Path is established by the identification of a protection switch or node and an end point switch or node in the MPLS network. The protection switch element ("PSL") initiates the setup of the working LSP and elements and the recovery LSP and elements. **It is also responsible for storing information about which network switch elements or portions thereof have protection enabled, and for maintaining a binding between outgoing labels specifying the working path and the protection/recovery path**. The latter enables the switchover to the recovery path upon the receipt of a protection switch trigger.

*Owens*, col. 11, ll. 2-12 (emphasis added). As shown above, the cited section of *Owens* describes how *Owens* binds work LSPs to protection LSPs; it does not say anything regarding the type of protection mode used, such as a 1+1 or a 1:1 protection mode. Thus, *Owens's* col. 11, ll. 2-12 fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP.

The Examiner also initially asserted that *Jain's* paragraphs 21 and 106 disclose label binding information comprising a protection mode. *See Final Office Action*, p. 11. However, **the cited sections of *Jain* fail to disclose that the fault notification message contains any label binding information**, much less the protection mode:

> The network may be a label-switching network. Label switching may be performed in accordance with MPLS. Propagation of a fault notification label may be by an interior gateway protocol (IGP). Propagation of the fault notification may include sending the fault notification by a label switched packet. The label switched packet may have a fault information label (FIL) that distinguishes the fault notification from data traffic. A substantially same FIL may be sent with each fault notification regardless of which network node originates the fault notification. Or, each network node may originate fault notifications having a FIL that is unique to the node. Network nodes that would be affected by the corresponding point of failure may store the indicia of the identified possible points of failure. The network nodes that would be affected by the corresponding point of failure may set up a label-switched path that uses a resource identified by the corresponding point of failure. At least one of the network nodes that receives a fault notification that corresponds to a point of failure that affects operation of the node may recover from the fault.
>
> Then, program flow moves to a state 906 in which a level or type of protection criteria for the resource identified in the state 904 may be specified. This criteria may, for example, specify a level of redundancy available to the resource. The level or kind of criteria specified in the state 906 will generally result from the topology of the network and from characteristics of individual network elements. For example, the protection provided may be 1:1, 1:n, 1+1, ring, or fast re-route. Fast re-route may be as explained above in reference to FIGS. 6-8 or another fast re-routing technique. Further, these criteria may be further specified according to classes and sub-classes of protection. For example, 1:1 protection may be considered a special case of 1:n protection that provides a higher level of fault tolerance than other 1:n levels.

*Jain*, ¶¶ 21 & 106. As shown above, the cited sections of *Jain* fail to disclose any messages comprising the protection mode. Thus, *Jain's* paragraphs 21 and 106 fail to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the type of LSP.

Subsequently, the Examiner asserted that *Owens's* col. 14, ll. 47-60 discloses that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the protection mode. *See Advisory Action*, p. 2. However, the cited section of *Owens* merely describes that the protection path is not used (i.e., keep in standby mode) until needed:

> By continuously sending an upstream message indicating that downstream traffic arrives at its destination, recovery time required to recover from the fault of a media link or a switching system can be minimized. If the switch status message used to indicate a functionality of a switch or a link is sent promptly enough, and to the appropriate node in a mesh network such as that shown in FIG. 1, the time required to reroute data messages between first and second endpoint switches over an alternate data path can be minimized. In the preferred embodiment, the alternate or so called protection path is preferably set up in advance and maintained in a stand by mode such that it is immediately available when required by the protection switch that will reroute data over the protection path.

*Owens*, col. 14, ll. 47-60 (emphasis added). As shown above, the cited section of *Owens* merely describes that the protection path is not used (i.e., keep in standby mode) until needed, not that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the protection mode. Thus, *Owens* fails to disclose that a first message from the PSL to the PML, a second message from the PML to the PSL, and a notification message transmitted by the PSL all comprise the protection mode. *Lewis* and *Jain* fail to make up for the shortcomings in *Owens*. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose at least one limitation of claims 1 and 3, and consequently fails to render obvious claims 1-19.

**F. The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 2 and 9-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose designating the PML router and the protection mode of the work LSPs at the PSL switched router.**

In addition to the reasons provided above, the combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 2 and 9-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose designating the PML router and the protection mode of the work LSPs at the PSL switched router. Claim 2 reads:

> 2. The method according to claim 1, further comprising: before creating the work LSP, **designating the PML router and the protection mode of the work LSPs at the PSL switched router**; or, after creating the work LSP, **designating the PML router and the protection mode of the work LSPs at the PSL switched router.**

(Emphasis added). As shown above, claim 2 requires designating the PML router and the protection mode of the work LSPs at the PSL switched router. The Examiner contends that *Jain's* paragraphs 13 and 85 disclose designating the PML router and the protection mode of the work LSPs at the PSL switched router. *See Final Office Action*, p. 8. While the cited section of *Jain* discloses that a protection LSP may be defined, it fails to disclose that the PML router is designated or the protection mode of the work LSPs at the PSL switched router (e.g., 1+1 protection or 1:1 protection):

> Each router may then store the SRLGs that relate to its own possible points of failure and those that relate to possible points of failure in other portions of the network. For example, each router may store only the SRLGs that correspond to resources within the network that the particular router is using to send data, e.g., those resources being used by label-switched paths (LSPs) set up by that router.
>
> Initially, **one or more protection LSPs is defined**. Each of these LSPs extends from a node in the network to another node that is at least two hops away, though two is the preferred number of hops. Thus, the protection LSP provides an alternate route between a first node and second node and avoids a third node that is between the first and second node. In addition, one or more protection LSPs may also be defined for the reverse path, i.e. for data traveling from the second node to the first node.

*Jain*, ¶¶ 13 & 85 (emphasis added). As shown above, the cited sections of *Jain* disclose that a protection LSP may be defined. However, the cited section of *Jain* fails to disclose that the PML router is designated or the protection mode of the work LSPs at the PSL switched router (e.g., 1+1 protection or 1:1 protection). *Lewis* and *Owens* fail to make up for the shortcomings in *Jain*. Thus, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose designating the PML router and the protection mode of the work LSPs at the PSL switched router. As such, the combination

of *Lewis*, *Jain*, and *Owens* fails to disclose all of the elements of claims 2, and consequently, fails to render obvious claims 2 and 9-14.

### G. The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because *Jain* fails to disclose that the steps in claim 10 are performed after the PML router receives the notification message.

In addition to the reasons provided above, the combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the steps in claim 10 are performed after the PML router receives the notification message. Claim 10 reads:

> 10. The method according to claim 9, **after the PML router receives the notification message,** if it is determined that the protection is in the 1:1 mode and it is chosen to create the return LSP dynamically via signaling, further comprising:
>
> the PML router transmitting to the PSL router a third message of requesting for creating the return LSP, with the binding information included in the third message;
>
> the PSL router assigning a label for the return LSP according to the third message, and returning a fourth message which comprises the binding information;
>
> the PML router binding the work LSP and the return LSP based on the binding information of the fourth message, and transmitting to the PSL router a notification message which comprises the binding information; the PSL router binding the work LSP and the return LSP based on the binding information of the notification message.

(Emphasis added). As shown above, claim 10 requires that the steps in claim 10 are performed after the PML router receives the notification. The Examiner contends that *Jain's* paragraphs 50 and 106 disclose that the steps in claim 10 are performed after the PML router receives the notification. *See Final Office Action*, pp. 14-15. However, the cited sections of *Jain* fail to disclose when the steps in claim 10 occur relative to receipt of the notification message:

> The PHY 304 may provide an interface directly to the transmission media 302 (e.g., the network links of FIG. 1). The PHY 304 may also perform other functions, such as serial-to-parallel digital signal conversion, synchronization, non-return to zero (NRZI) decoding, Manchester decoding, 8B/10B decoding, signal integrity verification and so forth. The specific functions performed by the PHY 304 may depend upon the encoding scheme utilized for data transmission. For example, the PHY 604 may provide an optical interface for optical links within the domain 100 (FIG. 1) or may provide an electrical interface for links to equipment external to the domain 100.
>
> Then, program flow moves to a state 906 in which a level or type of protection criteria for the resource identified in the state 904 may be specified. This criteria may, for example, specify a level of redundancy available to the resource. The level or kind of criteria specified in the state 906 will generally result from the topology of the network and from characteristics of individual network elements. For example, the protection provided may be 1:1, 1:n, 1+1, ring, or fast re-route. Fast re-route may be as explained above in reference to FIGS. 6-8 or another fast re-routing technique. Further, these criteria may be further specified according to classes and sub-classes of protection. For example, 1:1 protection may be considered a special case of 1:n protection that provides a higher level of fault tolerance than other 1:n levels.

*Jain*, ¶¶ 50 & 106 (emphasis added). As shown above, the cited sections of *Jain* fail to disclose when the steps in claim 10 occur relative to receipt of the notification message. *Lewis* and *Owens* fail to make up for the shortcomings in *Jain*. Thus, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the steps in claim 10 are performed after the PML router receives the notification. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose all of the elements of claim 10, and consequently, fails to render obvious claims 10-14.

### H. The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the third message, the fourth message, and the notification message comprise binding information.

In addition to the reasons provided above, the combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the third message, the fourth message, and the notification message comprise binding information. Claim 10 reads:

> 10. The method according to claim 9, after the PML router receives the notification message, if it is determined that the protection is in the 1:1 mode and it is chosen to create the return LSP dynamically via signaling, further comprising:
>
> the PML router transmitting to the PSL router a third message of requesting for creating the return LSP, with **the binding information included in the third message**;
>
> the PSL router assigning a label for the return LSP according to the third message, and returning **a fourth message which comprises the binding information**;
>
> the PML router binding the work LSP and the return LSP based on the binding information of the fourth message, and transmitting to the PSL router **a notification message which comprises the binding information**; the PSL router binding the work LSP and the return LSP based on the binding information of the notification message.

(Emphasis added). As shown above, claim 10 requires that the third message, the fourth message, and the notification message comprise binding information. The Examiner contends that *Jain's* paragraphs 13 and 16 disclose that the third message, the fourth message, and the notification message comprise binding information. *See Final Office Action*, p. 15. However, the cited sections of *Jain* fail to disclose that the third message, the fourth message, and the notification message comprise binding information:

> Each router may then store the SRLGs that relate to its own possible points of failure and those that relate to possible points of failure in other portions of the network. For example, each router may store only the SRLGs that correspond to resources within the network that the particular router is using to send data, e.g., those resources being used by label-switched paths (LSPs) set up by that router.
>
> The label used for a fault notification may be referred to as a "fault information label" (FIL). Information from the FIL along with associated payload data allow other network components to identify a fault. A node receiving a packet having a FIL is informed by the presence of the FIL that the packet is a fault notification. Thus, the fault notification is distinguishable from normal data traffic.

*Jain*, ¶¶ 13 & 16. As shown above, the cited sections of *Jain* fails to disclose that the third message, the fourth message, and the notification message comprise binding information. *Lewis* and *Owens* fail to make up for the shortcomings in *Jain*. Thus, the combination *Lewis*, *Jain*, and

*Owens* fails to disclose that the third message, the fourth message, and the notification message comprise binding information. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose all of the elements of claim 10, and consequently, fails to render obvious claims 10-14.

### I. The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the PSL router assigns a label for the return LSP.

In addition to the reasons provided above, the combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that the PSL router assigns a label for the return LSP. Claim 10 reads:

> 10. The method according to claim 9, after the PML router receives the notification message, if it is determined that the protection is in the 1:1 mode and it is chosen to create the return LSP dynamically via signaling, further comprising:
>
> the PML router transmitting to the PSL router a third message of requesting for creating the return LSP, with the binding information included in the third message;
>
> **the PSL router assigning a label for the return LSP** according to the third message, and returning a fourth message which comprises the binding information;
>
> the PML router binding the work LSP and the return LSP based on the binding information of the fourth message, and transmitting to the PSL router a notification message which comprises the binding information; the PSL router binding the work LSP and the return LSP based on the binding information of the notification message.

(Emphasis added). As shown above, claim 10 requires that the PSL router assigns a label for the return LSP. The Examiner contends that *Jain's* paragraphs 13 and 16 disclose that the PSL router assigns a label for the return LSP. *See Final Office Action*, p. 15. However, the cited sections of *Jain* fail to disclose that the PSL router assigns a label for the return LSP:

> Each router may then store the SRLGs that relate to its own possible points of failure and those that relate to possible points of failure in other portions of the network. For example, each router may store only the SRLGs that correspond to resources within the network that the particular router is using to send data, e.g., those resources being used by label-switched paths (LSPs) set up by that router.

> The label used for a fault notification may be referred to as a "fault information label" (FIL). Information from the FIL along with associated payload data allow other network components to identify a fault. A node receiving a packet having a FIL is informed by the presence of the FIL that the packet is a fault notification. Thus, the fault notification is distinguishable from normal data traffic.

*Jain*, ¶¶ 13 & 16. As shown above, the cited sections of *Jain* fail to disclose that the PSL router assigns a label for the return LSP. *Lewis* and *Owens* fail to make up for the shortcomings in *Jain*. Thus, the combination *Lewis*, *Jain*, and *Owens* fails to disclose that the PSL router assigns a label for the return LSP. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose all of the elements of claim 10, and consequently, fails to render obvious claims 10-14.

### J. The combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that both the PSL router and PML router bind the work LSP and the return LSP based on the binding information.

In addition to the reasons provided above, the combination of *Lewis*, *Jain*, and *Owens* fails to render obvious claims 10-14 because the combination of *Lewis*, *Jain*, and *Owens* fails to disclose that both the PSL router and PML router bind the work LSP and the return LSP based on the binding information. Claim 10 reads:

> 10. The method according to claim 9, after the PML router receives the notification message, if it is determined that the protection is in the 1:1 mode and it is chosen to create the return LSP dynamically via signaling, further comprising:
>
> the PML router transmitting to the PSL router a third message of requesting for creating the return LSP, with the binding information included in the third message;
>
> the PSL router assigning a label for the return LSP according to the third message, and returning a fourth message which comprises the binding information;
>
> **the PML router binding the work LSP and the return LSP based on the binding information** of the fourth message, and transmitting to the PSL router a notification message which comprises the binding information; **the PSL router binding the work LSP and the return LSP based on the binding information** of the notification message.

(Emphasis added). As shown above, claim 10 requires that both the PSL router and PML router bind the work LSP and the return LSP based on the binding information. The Examiner contends that *Jain's* paragraphs 13 and 16 disclose that both the PSL router and PML router bind the work LSP and the return LSP based on the binding information. *See Final Office Action*, p. 15. However, the cited sections of *Jain* fail to disclose that both the PSL router and PML router bind the work LSP and the return LSP based on the binding information:

> Each router may then store the SRLGs that relate to its own possible points of failure and those that relate to possible points of failure in other portions of the network. For example, each router may store only the SRLGs that correspond to resources within the network that the particular router is using to send data, e.g., those resources being used by label-switched paths (LSPs) set up by that router.
>
> The label used for a fault notification may be referred to as a "fault information label" (FIL). Information from the FIL along with associated payload data allow other network components to identify a fault. A node receiving a packet having a FIL is informed by the presence of the FIL that the packet is a fault notification. Thus, the fault notification is distinguishable from normal data traffic.

*Jain*, ¶¶ 13 & 16. As shown above, the cited sections of *Jain* fail to disclose that both the PSL router and PML router bind the work LSP and the return LSP based on the binding information. *Lewis* and *Owens* fail to make up for the shortcomings in *Jain*. Thus, the combination *Lewis*, *Jain*, and *Owens* fails to disclose that both the PSL router and PML router bind the work LSP and the return LSP based on the binding information. As such, the combination of *Lewis*, *Jain*, and *Owens* fails to disclose all of the elements of claim 10, and consequently, fails to render obvious claims 10-14.

## VIII. CONCLUSION

In view of the above arguments, the Appellant respectfully requests that the rejection of the claims be reversed and the case advanced to issue. If the Examiner feels that a telephone interview would advance prosecution of the instant application, then the Appellant invites the Examiner to call the attorneys of record.

The Commissioner is hereby authorized to charge payment of any further fees associated with any of the foregoing papers submitted herewith, or to credit any overpayment thereof, to Deposit Account No. 50-1515, of Conley Rose, P.C. of Texas.

Respectfully submitted,
CONLEY ROSE, P.C.

Date: 2/15/2011

Landon E. Wiebusch
Reg. No. 65,145

ATTORNEY FOR APPELLANT

5601 Granite Parkway, Suite 750
Plano, Texas 75024
Telephone: (972) 731-2288
Facsimile: (972) 731-2289

## IX. CLAIMS APPENDIX

The text of the claims involved in the appeal is:

1. A method for binding a work label switching path (LSP) with a protection LSP, comprising:

a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML) to request for creating the protection LSP of the work LSP;

the PML router assigning a label for the protection LSP based on the first message, and returning a second message which comprises the binding information;

upon receiving the second message, the PSL router binding the work LSP with the protection LSP according to the binding information, and transmitting a notification message which comprises the binding information to the PML switched router; and

the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,

wherein the binding information comprises an identifier of the work LSP, a type of the LSP, and a protection mode, and

wherein the PSL and PML are label edge routers.

2. The method according to claim 1, further comprising: before creating the work LSP, designating the PML router and the protection mode of the work LSPs at the PSL switched router; or, after creating the work LSP, designating the PML router and the protection mode of the work LSPs at the PSL switched router.

3. A method for binding a work label switching path (LSP) with a protection LSP, comprising:

in the process of creating the protection LSP, a Path Switching Label Switching Router (PSL) transmitting a first message which comprises a binding information to a Path Merging Label Switching Router (PML) to request for creating the protection LSP of the work LSP;

the PML router assigning a label for the protection LSP based on the first message, and returning a second message which comprises the binding information;

upon receiving the second message, the PSL router binding the work LSP with the protection LSP according to the binding information, and transmitting a notification message which comprises the binding information to the PML switched router; and

the PML router binding the work LSP with the protection LSP according to the binding information in the notification message,

if the protection mode for the work LSPs is 1+1 mode, the binding information comprises the work LSP identifier, LSP type, and the protection mode; and

if the protection mode for the work LSPs is 1:1, the binding information comprises the work LSP identifier, LSP type, the protection mode and selection mode of the return LSP in the 1:1 protection mode.

4. The method according to claim 19, further comprising, after the PML router receives the notification message, if it is determined that the protection is in the 1:1 mode and it is chosen to create the return LSP dynamically via signaling:

the PML router transmitting to the PSL router a third message of requesting for creating the return LSP, with the binding information included in the third message;

the PSL router assigning a label for the return LSP according to the third message, and returning a fourth message which comprises the binding information;

the PML router binding the work LSP and the return LSP based on the binding information of the fourth message, and transmitting to the PSL router a notification message which comprises the binding information;

the PSL router binding the work LSP and the return LSP based on the binding information of the notification message.

5. The method according to claim 4, wherein, if Resource Reservation Protocol (RSVP) is used to create the LSP, the first message and the third message are path messages in the RSVP, and the second message and the fourth message are Resv messages in the RSVP, and the notification message is Reservation Configuration (ResvConf) message in the RSVP.

6. The method according to claim 5, further comprising: extending a binding object in the RSVP, and extending the Path message, Resv message and ResvConf message to comprise information of the binding object to implement the binding of the work LSP and the protection LSP.

7. The method according to claim 4, wherein, if label distribution protocol (LDP) or constraint route-label distribution protocol (CR-LDP) is used to create the LSP, the first message and the third message are the Label Request messages of the LDP or CR-LDP, and the second message and the fourth message are the Label mapping messages of the LDP or the CR-LDP, and the notification message is a notification message in the LDP or the CR-LDP.

8. The method according to claim 7, further comprising: extending the binding Type Length Value (TLV) in the LDP or the CR-LDP, and adding the binding TLV to the Label Request message, Label mapping message and notification message to implement the binding of the work LSP and the protection LSP.

9. The method according to claim 2, if the protection mode for the work LSPs is 1+1 mode, the binding information comprises the work LSP identifier, LSP type, and the protection mode; if the protection mode for the work LSPs is 1:1, the binding information comprises the work LSP identifier, LSP type, the protection mode and selection mode of the return LSP in the 1:1 protection mode.

10. The method according to claim 9, after the PML router receives the notification message, if it is determined that the protection is in the 1:1 mode and it is chosen to create the return LSP dynamically via signaling, further comprising:

the PML router transmitting to the PSL router a third message of requesting for creating the return LSP, with the binding information included in the third message;

the PSL router assigning a label for the return LSP according to the third message, and returning a fourth message which comprises the binding information;

the PML router binding the work LSP and the return LSP based on the binding information of the fourth message, and transmitting to the PSL router a notification message which comprises the binding information; the PSL router binding the work LSP and the return LSP based on the binding information of the notification message.

11. The method according to claim 10, wherein, if the RSVP is used to create the LSP, the first message and the third message are path messages in the RSVP, and the second message and the fourth message are Resv messages in the RSVP, and the notification message is ResvConf message in the RSVP.

12. The method according to claim 11, further comprising: extending a binding object in the RSVP, and extending the Path message, Resv message and ResvConf message to comprise information of the binding object to implement the binding of the work LSP and the protection LSP.

13. The method according to claim 10, wherein, if the LDP or the CR-LDP is used to create the LSP, the first message and the third message are the Label Request messages of the LDP or CR-LDP, and the second message and the fourth message are the Label mapping messages of the LDP or the CR-LDP, and the notification message is a notification message in the LDP or the CR-LDP.

14. The method according to claim 13, further comprising: extending the binding the TLV in the LDP or the CR-LDP, and adding the binding TLV to the Label Request message, Label mapping message and notification message to implement the binding of the work LSP and the protection LSP.

15. The method according to claim 1, wherein data is transmitted via the work LSP and protection LSP simultaneously from PSL to PML, the PML receives the data from the work LSP in normal conditions, if there is a failure in the work LSP, the PML receives data from the protection LSP.

16. The method according to claim 1, wherein the binding occurs during creation of the protection LSP.

17. The method according to claim 16, wherein at least one node in the protection LSP is not part of the work LSP.

18. The method according to claim 17, wherein data is transmitted via the work LSP and protection LSP simultaneously from PSL to PML, the PML receives the data from the work LSP in normal conditions, if there is a failure in the work LSP, the PML receives data from the protection LSP.

19. The method according to claim 1, if the protection mode for the work LSPs is 1:1, the binding information comprises the work LSP identifier, LSP type, the protection mode and selection mode of the return LSP in the 1:1 protection mode, and wherein the PSL and PML are label edge routers.

## X. EVIDENCE APPENDIX

None.

## XI. RELATED PROCEEDINGS APPENDIX

None.